AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the Facebook User ID 100025030299143 that is stored at premises controlled by Facebook Inc.

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2339B	Providing or Attempting to Provide Material Support and Resources to a Foreign Terrorist Organization

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

P. Andrew Gragan, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/3/18

Judge's signature

City and state: Dayton, Ohio

Michael J. Newman, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, P. Andrew Gragan, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), United States Department of Justice, Cincinnati Division. I have been employed as a Special Agent with the FBI since May 2016. I have received training in national-security investigations and criminal investigations, and I have conducted investigations related to international terrorism, domestic terrorism, white-collar crimes, drug trafficking, public corruption, and violent crimes. As part of these investigations, I have participated in physical surveillance and records analysis, worked with informants, conducted interviews, served court orders and subpoenas, and executed search warrants.

2. I make this affidavit in support of an application for a search warrant for information associated with Facebook user ID **100025030299143** ("SUBJECT ACCOUNT"), that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

3. Based on my training and experience, and the facts as set forth in this affidavit, I submit there is probable cause to believe that violations of 18 U.S.C. § 2339B (providing and attempting to provide material support and resources to a foreign-terrorist organization) have

been committed by **NASER ALMADAOJI** ("**ALMADAOJI**") and there is probable cause to believe that evidence, fruits, and instrumentalities of these violations, as described more particularly in Attachment B, are present within the information associated with the SUBJECT ACCOUNT.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause and does not set forth all of my knowledge about this matter.

JURISDICTION

5. This court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL STATUTES AND DESIGNATIONS

6. Title 18, United States Code, Section 2339B, prohibits, in pertinent part, a person from knowingly providing "material support or resources to a foreign terrorist organization," or attempting or conspiring to do the same.

7. The term "material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel…, and transportation, except medicine or religious materials." 18 U.S.C. Section 2339A(b)(1) and Section 2339B(g)(4). Section 2339B(h) provides that "[n]o person may be

prosecuted under this section in connection with the term 'personnel' unless that person has knowingly provided, attempted to provide, or conspired to provide a foreign terrorist organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct that operation of that organization. Individuals who act entirely independent of the foreign terrorist organization to advance its goals or objectives shall not be considered to be working under the foreign terrorist organization's direction and control."

8. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq ("AQI"), then known as Jam 'at al Tawid wa' al-Jahid, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive order 13224.

9. On or about May 15, 2014, the Secretary of State amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham ("ISIS"—which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furquan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

BACKGROUND INFORMATION

Definitions

10. The following definitions apply to this Affidavit, including all attachments to the Affidavit:

a. "**Internet Service Providers**" or "**ISPs**" are commercial organizations that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

b. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four

sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

c. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

d. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

11. According to Immigration and Customs Enforcement, **NASER ALMADAOJI (ALMADAOJI)** is a 19-year-old individual who was born in Iraq and is a naturalized U.S. citizen. **ALMADAOJI** resides in Beavercreek, Ohio, within the Southern District of Ohio.

FOREIGN TRAVEL AND CBP INTERVIEW

12. Between approximately February 16, 2018, and February 24, 2018, **ALMADAOJI** traveled outside of the United States to the countries of Egypt and Jordan.

13. On or about February 24, 2018, United States Customs and Border Protection ("CBP") interviewed **ALMADAOJI** upon his re-entry into the United States. **ALMADAOJI** made the following statements during the interview, among others:

a. **ALMADAOJI** claimed to have traveled by himself and that he traveled to Jordan and Egypt.

b. **ALMADAOJI** stated that, when in Jordan, he traveled to Irbid, Amman, and to the Israeli border to "see the land that was taken from Jordan." **ALMADAOJI** claimed he chose to go to Jordan and Cairo, Egypt, because they looked "nice," but he would not elaborate.

c. **ALMADAOJI** advised CBP that he had only two friends, and he only talks to two people outside of work, but they are not "religious enough" for him. **ALMADAOJI** advised CBP that he told his family he was going overseas, but he did not tell them when he was coming back to the United States.

d. **ALMADAOJI** stated he returned to the United States after a taxi driver took off with his backpack and $3000. He claimed that he reported the incident to the U.S. Embassy.

e. **ALMADAOJI** advised CBP that at one time he was interested in joining the Marine Corps, but he lost interest because he "became religious" and had "different political views." **ALMADAOJI** claimed that he had been searching for the "purpose of life" and started focusing on religion. **ALMADAOJI** had come to the conclusion that his purpose was to serve Allah by any means possible.

f. **ALMADAOJI** referenced U.S. airstrikes that killed Muslims and stated the United States needed to leave the Middle East. **ALMADAOJI** stated he thought about joining the Peshmergan military forces in northern Iraq, but he decided against it. He stated the Peshmergan forces were the "real forces in Iraq to stop ISIS, not U.S."

g. **ALMADAOJI**, when asked about his views on ISIS, stated ISIS was "bad for killing other Muslims," but that most Muslims killed by ISIS were "Shiites." **ALMADAOJI** stated he is "Sunni" so "Shiites were their natural adversaries." When asked why he felt like that, he answered "they didn't follow true Islam" and stated Iraq was a mess right now and the Iraqi government was corrupt and a joke,

and that the people of Iraq were no freer now than they were before ISIS invaded Iraq.

14. During the interview, CBP observed approximately four shemagh-style head wraps in **ALMADAOJI**'s bag. When CBP asked about the shemaghs, **ALMADAOJI** responded he liked the way they looked on "fighters." He was asked if he had seen any fighters while he was in Egypt or Jordan. **ALMADAOJI** stated, "no not really," but that he sees fighters wearing shemaghs online all the time.

SUBJECT FACEBOOK ACCOUNT

15. During the February 24, 2018, interview, **ALMADAOJI** provided CBP with his email address—nasermunshid16@gmail.com. **ALMADAOJI** also provided (937) 969-0509 as his telephone number.

16. On or about May 10, 2018, Google LLC provided a response to a subpoena served on or about May 10, 2018, for nasermunshid16@gmail.com. In the response, Google LLC provided subscriber information for nasermunshid16@gmail.com, including the name "Abu Ahmad;" phone number (937) 969-0509 as the SMS number associated with the account; and recovery email address of abubadraliraqi@gmail.com. The phone number related to nasermunshid16@gmail.com is the same phone number provided by **ALMADAOJI** to CBP. The IP address information provided by Google shows that an individual logged into nasermunshid16@gmail.com from IP addresses resolving to locations in Amman, Jordan; Cairo, Egypt; and Giza, Egypt, between approximately February 16, 2018, and February 22, 2018—the time when **ALMADAOJI** traveled overseas to Jordan and Egypt.

17. On or about June 4, 2018, Google LLC provided a response to a subpoena served on or about May 14, 2018, for abubadraliraqi@gmail.com. In the response, Google LLC provided subscriber information for abubadraliraqi@gmail.com, including the name "Abu

Muhammad al Iraqi," as well as IP address and log-in information. The IP address information provided by Google shows that abubadraliraqi@gmail.com was logged into from IP addresses resolving to locations in Amman, Jordan; Cairo, Egypt; and Giza, Egypt, between approximately February 16, 2018, and February 22, 2018—the time when **ALMADAOJI** traveled overseas to Jordan and Egypt.

18. On or about June 18, 2018, PayPal identified four accounts under the name **ALMADAOJI**. Three of those accounts listed (937) 969-0509 as the contact number—that is, the same number **ALMADAOJI** identified as his contact number when talking with CBP and the same number associated with email accounts purportedly relating to **ALMADAOJI**. PayPal also identified the same address as that listed for **ALMADAOJI** in the records of the Ohio Bureau of Motor Vehicles ("BMV").

19. On or about July 3, 2018, Facebook provided a response to a subpoena served on or about June 21, 2018, which sought account information associated with the email address abubadraliraqi@gmail.com. In the response, Facebook provided subscriber information for an account associated with abubadraliraqi@gmail.com, including the name "Abu Muhammad," the user identity (UID) **100025030299143** (SUBJECT ACCOUNT), and a registration IP address of 75.186.47.208. The name "Abu Muhammad" associated with the SUBJECT ACCOUNT is similar to the name "Abu Muhammad al Iraqi" associated with the abubadraliraqi@gmail.com email address. The Facebook subpoena information indicated the SUBJECT ACCOUNT was registered on March 21, 2018.

20. On or about July 9, 2018, a preservation request was submitted to Facebook, which is set to expire on or about December 6, 2018, and which requested that Facebook preserve information related to the SUBJECT ACCOUNT.

21. On or about July 26, 2018, Charter Communications, Inc. provided response to a subpoena served on or about July 11, 2018, which sought information related to **ALMADAOJI**'s name, as well as **ALMADAOJI**'s address on N. Fairfield Road, in Beavercreek, Ohio. In the response, Charter Communications, Inc. provided subscriber and account information related to the address. The information provided shows that a Charter Communications, Inc. account is subscribed to an individual believed to be **ALMADAOJI**'s father at the N. Fairfield Road address. The records show that the IP address 75.186.47.208 is associated with the account. This is the same IP address used to register the SUBJECT ACCOUNT, as discussed above in paragraph 19, above.

22. On or about July 27, 2018, Facebook provided a response to a court order under 18 U.S.C. § 2703(d), served on or about July 12, 2018, which sought information related to the SUBJECT ACCOUNT. In the response, Facebook provided subscriber information for the SUBJECT ACCOUNT, which corresponded to the information received from the subpoena discussed in paragraph 19, above. The information was similar to that provided by the aforementioned subpoena that was responded to on or about July 3, 2018. Also included in the information was an additional registered email account of thevader30@gmail.com, and information, include date, time, and author, related to messages (without content) between the user of the SUBJECT ACCOUNT and another Facebook user. Subscriber information received from Google LLC regarding the email address thevader30@gmail.com indicated a subscriber name of "Fabiano Trappo." Open source information shows that IP addresses used to log into the thevader30@gmail.com resolve to Italy.[1]

[1] It should be noted that on or about July 27, 2018, Sony Interactive Entertainment LLC responded to a subpoena that requested information for a Sony Model PS4 with serial number of MB325342632. Information provided shows that the following email addresses, among others,

MESSAGING APPLICATION COMMUNICATIONS

23. Open-source research revealed that **ALMADAOJI**'s phone number, (937) 969-0509, was registered to a publically-available encrypted messaging application with a specific and unique user-identity number. The unique user-identity number was associated with the username @AbuMuhammad16, with a display name (in Arabic) of "Abu Muhammad al-Iraqi." "Abu Muhammad al Iraqi" is the same general name connected to abubadraliraqi@gmail.com, as discussed in paragraph 17 above.

24. Based on reporting from a confidential human source ("CHS"), the user name @AbuMuhammad16 was changed to @AbuMuhammad19 in or around July 2018. The unique user-identity number for @AbuMuhammad19 was confirmed to be the same unique number as that specified for @AbuMuhammad16.

25. Between on or about August 5, 2018, and on or about August 19, 2018, an individual using the encrypted messaging account @AbuMuhammad19, believed to be **ALMADAOJI**, based on the above information, exchanged messages with an undercover employee ("UCE"). The UCE and the individual communicating through the username @AbuMuhammad19 discussed using encrypted messaging applications and other social-media platforms. When the individual was asked by the UCE if the individual knew of other trusted and

---

have been used as sign-in IDs for the Sony Model PS4 with serial number MB325342632: nasermunshid16@gmail.com, abubadraliraqi@gmail.com, and thevader30@gmail.com. Information obtained from PayPal shows that the Sony Model PS4 with serial number of MB325342632 was purchased on March 10, 2018, using a PayPal account registered to the nasermunshid16@gmail.com email address, and was shipped to "Naser Almadaoji" at his address on N. Fairfield Road in Beavercreek, Ohio.

secured sites to read "dawla news," the individual replied that he/she was not aware of sites besides "nashir news."[2]

26. On August 19, 2018, in a group chat room, the UCE and the individual using the @AbuMuhammad19, along with two other users, exchanged messages regarding the use of thermal imaging on borders and possible ways to avoid detection from thermal-imaging devices. In a one-on-one chat the same day, the individual offered to help the UCE after the UCE explained that he/she was attempting to help a friend cross the border out of Sham[3] and into Turkey. The UCE explained that his/her friend lacks monetary resources. The individual using the account associated with **ALMADAOJI** offered to ask around, noting that Sham is a "difficult place and contacts are weak at the moment." The individual also cautioned that "leaving sham to go back home is seen as treason in most cases and I don't know how the brothers are gonna take it if i tell them that."

27. On or about August 15, 2018, the individual using the encrypted messaging account @AbuMuhammad19 communicated in English with an FBI confidential human source who was posing as a France-based contact (hereinafter referred to as Contact #1). During the conversation, the individual informed Contact #1 that he was from Iraq and previously lived in Southern Iraq "with majority shia pigs" before leaving in 2006. The individual stated that the Shia were "everywhere, they're kicking Ahul al Sunnah from their homes in North Baghdad,

---

[2] Based on my training and experience, and information from other agents, I know the term "dawla" (or "dawlah") refers to the Islamic State. I also know that the Nashir News Agency is a propaganda outlet for ISIS.

[3] Based on my training and experience, and information from other agents, I know that "Sham" refers to the Levant, a geographic area comprised of Syria, Lebanon, Palestine, and Jordan. I also know that it is commonly used as short-hand to refer to the portions of Syria where ISIS is known to operate.

Diyala, Salah al Din and other places so they take their homes and spread their filth all over Iraq." In response to a video that Contact #1 posted during the conversation, which depicted ISIS combat operations in Syria, the individual stated "Alhamdulallah."

28. On August 16, 2018, the individual using the @AbuMuhammad19 account informed Contact #1 that he recently finished high school, was looking for a job, and was not interested in attending university since he was "not planning to stay in this land much longer." Contact #1 asked the individual if he was referring to a path for hijra[4] and the individual responded, "Yes, akhi but I make dua and take every heed there is and Allah Subhanahu wa Ta'ala will find a way for His sincere servants." Contact #1 offered to put the individual in contact with, who the individual believed to be, a British brother in Iraq who "has helped an old friend of me get to khurassan."[5] In response, the individual stated "anything you have is great."

29. On August 16, 2018, the individual using the encrypted messaging account @AbuMuhammad19, believed to be **ALMADAOJI**, engaged in conversation with the same FBI confidential human source (that is, the source serving as Contact #1), but the source was now posing as a totally separate person—that being the Iraq-based British contact referenced above in paragraph 27 (hereinafter referred to as Contact #2). During the conversation, the individual using the encrypted messaging application told Contact #2 that he recently met Contact #1 on the messaging application and discussed hijra. At Contact #2's suggestion, Contact #2 and the individual believed to be **ALMADAOJI** moved the conversation to a secret chat. During the

---

[4] Based on my training and experience, and information from other agents, I know that "Hijra" or "Hijrah" is a term that originally referred to Muhammad's movement from Mecca to Medina. I also know that the term "hijrah" more recently has been used to refer to traveling from the West to ISIS territory.

[5] Based on my training and experience, and information from other agents, I know that "khurassan" is a term used to refer to ISIS affiliates in Afghanistan.

secret chat, the individual believed to be **ALMADAOJI** told Contact #2 that he was not yet ready for hijra, but he was trying to assist a brother in Egypt who was being forced into the Egyptian military in approximately one month. The individual believed to be **ALMADAOJI** stated "I know wilayat Sinai[6] is not possible at the moment" and inquired "is there a way to Libya or anywhere near egypt."

30. When Contact #2 inquired why the individual believed to be **ALMADAOJI** was not yet ready for hijra, the individual stated "Right now my problem is money." The individual believed to be **ALMADAOJI** also told Contact #2 that he was currently in the United States and that he keeps "a low profile." The individual believed to be **ALMADAOJI** stated: "I want sham but that's not possible currently but maybe a few months from now when I'm ready." When asked by Contact #2 who he supported, or who he was trying to join, the individual believed to be **ALMADAOJI** demonstrated operational security by refusing to say exactly who he intended to support when traveling overseas. Rather, the individual stated, "Lol who goes by wilayat" and "I just don't like to formally say it just in case the authorities here get their hands on these conversations." When Contact #2 told him that Contact #2 has "spoken to brothers who think I'm AQ" (referring to Al-Qaeda), the individual believed to be **ALMADAOJI** responded "Lol no not those guys." Contact #2 asked the individual believed to be **ALMADAOJI** why he wanted to make hijra and suggested that "[m]any brothers will say that you are in the best place

[6] Based on my training and experience, and information from other agents, I know that "Wilayat" translates to "State." In context, **ALMADAOJI**'s use of the phrase "Wilayat Sinai" refers to ISIS affiliates located in the Sinai Peninsula. The Department of States lists "Wilyat Sinai" as an "aka" of Ansar Bayt al-Maqdis ("ABM"), or ISIL Sinai Province ("ISIL-SP"). ABM was designated as a Foreign Terrorist Organization originally on April 9, 2014. According to the Department of State, in November 2014, ABM officially declared allegiance to ISIL. In September 2015, the Department of State amended ABM's designation to add the primary name ISIL Sinai Province.

for jihad." The individual responded by saying "I don't like where this is going . . . we'll stick to hijrah for now." After Contact #2 stated "I am not trying to push you towards anything I have no way of helping you with something in your own country," the individual believed to be **ALMADAOJI** stated: "I know this akhi but once there us [sic] hijra then there will jihad in the land of hijra. I don't like to keep traces back to me that's why I'm not saying somethings by name just incase I end up messaging the wrong person without knowing."

31. Between approximately August 18, 2018, and approximately August 20, 2018, the individual believed to be **ALMADAOJI** continued to message with Contact #2. During conversation on August 19, 2018, Contact #2 offered to connect the individual believed to be **ALMADAOJI** with "American brothers who have gone back" and who "often help brothers out." The individual responded, "That'll be great akhi ask around and let me know" and "Tell them north east us." When the individual believed to be **ALMADAOJI** inquired "why did they go back exactly," Contact #2 stated "Can't say…your only allowed to leave if the emir has something for you to do. Let's say that they have projects wherever they are." The individual believed to be **ALMADAOJI** responded, "Oh I see. I didn't mean to ask it that way." Contact #2 stated, "If any of these brothers do get in contact do not mention dawla. What they are doing has a lot of risk." The individual believed to be **ALMADAOJI** stated: "No akhi I am well aware of what's going on, that's why I'm not mentioning anything by name here."

32. On or about August 20, 2018, the individual believed to be **ALMADAOJI** discussed his Egyptian associate that was slated to be drafted into the Egyptian military in approximately two months. Contact #2 asked the individual believed to be **ALMADAOJI** how the Egyptian was and how much he trusted the Egyptian. The individual believed to be **ALMADAOJI** responded, "Alhamdulillah he's well" and "I trust him very well." The

individual went on to say, "Yea I been to egypt once and met him. I don't wanna say here why I was in egypt but him and I planned something and it didn't work at [sic] well." Contact # 2 inquired, "Ahh how you know wilaya Sinai is hard to reach?" The individual believed to be **ALMADAOJI** replied "Yea unfortunately I had to learn the hard way despite the fact I was talking to a brother and he told me that himself." When asked by Contact #2 if the brother had tricked him, the individual believed to be **ALMADAOJI** stated, "No akhi the brother warned me it was difficult to reach Sinai, I don't know if he was in the lands of Dawlah or just a munasir but no I didn't end up in prison either." The individual also stated that no one knows that he was in Egypt, but his family knows he was in Jordan since he was attempting to reach "dar'a"[7] a second time.

33. The individual believed to be **ALMADAOJI** offered to put Contact #2's associates in touch with the Egyptian. Contact #2 asked if the Egyptian was on the encrypted messaging application. The individual believed to be **ALMADAOJI** responded, "No Facebook." He then stated he did not know why the Egyptian was not on the encrypted messaging application and said, "I told him to come to [encrypted messaging application] but he rather stick to Facebook."

34. Contact #2 asked for the thoughts of the individual believed to be **ALMADAOJI** on "assisting with some projects in your own country." After Contact #2 clarified that he/she was talking about the United States, the individual believed to be **ALMADAOJI** stated it was a "big ask," and asked Contact #2 to "shed a little light on the type of projects." Contact #2 replied: "It is a big ask, you are not the kind of brother we would ask to take a knife to the street

[7] Dar'a, also known as Daraa, is a city in southern Syria, located approximately 18 miles east of Irbid, Jordan.

if you know what I mean. There are more important projects there that require intelligent brothers who are determined. I ask only if you would be willing or interested to contribute if hijra is not possible." The individual believed to be **ALMADAOJI** replied: "Of course I'm always willing."

35. On or about August 22, 2018, the individual believed to be **ALMADAOJI** continued to communicate in English with Contact #2. The individual turned the conversation toward the topic of United States politics and asked if Contact #2 stayed updated on the subject. Contact #2 told the individual, "I told some of the brothers here about you, they were very impressed and want you to send a bayyah,[8] two of our local leaders agreed to send you a video to [sic]." The individual believed to be **ALMADAOJI** stated: "In shaa Allah we will then proceed forward with it" and then stated: "But since our talk about projects in the west I did a lot of thinking and I imagined a scenario of the collapse of the US as a nation. They have a lot of weak spots 2 really weak spots that would ignite the deadliest civil war on earth if the right spots are poked." The individual believed to be **ALMADAOJI** stated the weak spots were "racial issues" and "militias." When Contact #2 asked if he was talking about starting a race war to destabilize the U.S., the individual believed to be **ALMADAOJI** replied, "Now let's talk theory and scenario" and proposed the following scenario:

> *Say someone wanted to convince the militias to start a war with the government They would need proof that the government is planning to end the milita movement which is a US citizen right by the constitution They could do that behind doors. Such as assassinating militia leaders and then blaming it on the government Or hacking into their devices, filling it with child sexual abuse videos, then tipping the fbi abd* [sic] *the militia leaders get thrown behind bar with atleast 20 years*

---

[8] Based on my training and experience, and information from other agents, I know that bayyah, bayyat, and bayat, are Arabic terms that mean pledge, or oath, of allegiance to a leader.

36. The individual believed to be **ALMADAOJI** then stated that "federal buildings" were "more sensitive for the militias to hit than police stations and military bases." The individual stated, "With a coordinated attack such as car bombings parked next to fed buildings with all the previous build we talked about. And there you have the US on its knees." The individual believed to be **ALMADAOJI** stated, "It may take a long time to pull something off but it's long term. This will divide the nation as a whole, including government, military and law enforcement." The individual told Contact #2, "If you were to mention this to anyone keep it close guarded circle."

37. On or about August 24, 2018, the individual believed to be **ALMADAOJI** also stated to Contact #2: "After thinking about it for sometime, these projects need secrecy, and lots of it. So there can't be any physical evidence that leads it back to the I.S."

38. On August 24, 2018, the FBI confidential source sent a video to the individual believed to be **ALMADAOJI** on the encrypted messaging application. Prior to sending the video, Contact #2 told the individual that "these two brothers have very important positions with us and there [sic] identity and voices must be protected and not shared." The individual believed to be **ALMADAOJI** then asked Contact #2, "So you told them about the whole plan or part of it?"

39. In the video, Contact #2 and another individual are representing themselves as Iraqi-based ISIS members. The individuals are wearing shemaghs and, what appears to be, both a rifle and knife are visible. In the video, the following, among other things, was stated in Arabic[9] to the individual believed to be **ALMADAOJI**:

[9] Any summaries of, or quotes from, Arabic communications referenced herein are based on preliminary translations.

I am your brother from the State of Islam, Wilayah Iraq, Abu Adhal al Tikreeti, with me here Abu Omar al Faransi who will accept your pledge bayyah to emir almoumeneen.[10]

In response to receiving the video, the individual believed to be **ALMADAOJI** stated: "A video has never made me smile with sincerity in a while. Give them glad tidings of bay'a tomorrow in shaa Allah." The individual believed to be **ALMADAOJI** then asked Contact #2 to "destroy [sic] the chat now. The one with the video" and suggested that Contact #2 "might wanna delete the video from your side."

40. On August 25, 2018, the individual believed to be **ALMADAOJI** communicated with Contact #2, stating "Although I did not get the project done. In shaa Allah expect a video coming soon today." The individual confirmed with Contact #2 whether he should send the video by way of the encrypted messaging application, stating "Let me know as soon as possible akhi, I'm about to go shoot the video soon." Contact #2 confirmed that the messaging application was "fine for the video." The individual believed to be **ALMADAOJI** then told Contact #2 that it would be tomorrow before he would send the video.

41. On or about August 26, 2018, the individual believed to be **ALMADAOJI** told Contact #2 that "Earlier when I tried to go do the video, I felt a sudden need for sleep, I had to force myself up to pray dhur and then went to sleep immediately after. There will be a spiritual struggle to get through with this akhi, I hope you understand if I take a little bit too long to get the video." Contact #2 replied: "Ok brother send when you can, today or tomorrow will be fine. Fighting here is starting to pick up so I want to make sure we get you in contact with the brothers soon that is my only concern. May Allah guide and facilitate you akhy." Later that day, the individual forwarded a video to Contact #2 via

[10] Emir almoumeneen translates to "Caliph of the Faithful" and, based on training and experience, and information from other agents, I know to be a title that refers to Abu Bakr al-Baghdadi, the self-proclaimed claimed leader of ISIS.

a separate secret chat session on the messaging application. In the video, a person believed to be **ALMADAOJI** is wearing a scarf that is wrapped in a manner that covers the person's head and lower face. Under the scarf, a black "beanie" style cap can be seen on the person's head. The person states the following in Arabic:

> *Praise be to God and peace and prayers be upon His messenger. I pledge allegiance to Sheikh Abu Bakr al-Baghdadi, the Caliph of the faithful, to obey his command in all situations, in difficulty and in prosperity, and not to dispute orders until I see a common disbelief of which I have a proof from God. God is the witness to what I am saying.*

42. During surveillance conducted between on or about May 14, 2018, and on or about September 7, 2018, FBI surveillance observed, on several occasions, **ALMADAOJI** wearing a black knit or "beanie" style cap consistent with the cap worn by the person depicted in the video.

43. On or about August 27, 2018, the individual believed to be **ALMADAOJI** told Contact #2 via the encrypted messaging application that he would not be able to travel to meet brothers currently in the United States and hoped they could pick him up. The individual told Contact #2 that the individual was located in Ohio.

44. Based on my training and experience, I am aware that individuals involved in attempting to provide, or providing, material support and resources to foreign-terrorist organizations often communicate with others involved in similar conduct via e-mail, social-media accounts such as Facebook, and online chat programs. I also know based on my training and experience that individuals associated with such activities use Facebook and other social media to watch videos and images relating to ISIS and other foreign-terrorist organizations. Those individuals obtain and share such videos and images with each other via a variety of means, including email, social-media accounts, and online-chat programs. Based on my training and experience, I know that individuals involved in material-support offenses often use multiple

accounts, aliases, and means to communicate. These multiple accounts or aliases are used as a means to avoid detection from law enforcement.

45. Based on my training and experience, I know that:

a. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

b. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

c. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

d. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

e. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

f. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a

user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

g. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

h. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

i. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

j. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

k. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The

activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

l. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

m. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

n. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

o. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

46. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

47. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

48. As detailed above, **ALMADAOJI** has used a messaging application to discuss matters related to ISIS, potential prospective terrorist activity, and sent a video purporting to pledge allegiance to the self-proclaimed claimed leader of ISIS. Moreover, during communications with Contact #2 on the messaging application, **ALMADAOJI** discussed his prior travel to Jordan and Egypt. **ALMADAOJI** discussed his interaction with an Egyptian associate in relation to that travel, and characterized his travel as a failed attempt to reach "Wilayat Sinai." **ALMADAOJI** told Contact #2 that his Egyptian associate used Facebook. Accordingly, based on the foregoing information in this affidavit, I submit there is probable cause to believe that violations of 18 U.S.C. § 2339B have been committed by **ALMADAOJI**, and that evidence, fruits, and instrumentalities of these violations are present within the information associated with the SUBJECT ACCOUNT.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

49. I anticipate executing the requested warrant for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Facebook to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I

of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

50. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. § 2339B (providing and attempting to provide material support and resources to a foreign terrorist organization) have been committed by **ALMADAOJI**, and that there is probable cause to believe that, present within the information associated with the SUBJECT ACCOUNT, as described more particularly in Attachment A, is evidence, fruits, and instrumentalities of these violations, as described more particularly in Attachment B.

51. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

52. Because the warrant for the account described in Attachment A will be served on Facebook, Inc., who will then compile the requested records at times convenient to that entity, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Special Agent P. Andrew Gragan
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 3rd day of October 2018.

HON. MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

This warrant applies to information associated with the Facebook user ID **100025030299143** (SUBJECT ACCOUNT) that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the SUBJECT ACCOUNT, listed in Attachment A:

a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities from August 1, 2017 to present;

c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from August 1, 2017 to present, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

d. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification

numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

e. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

f. All other records and contents of communications and messages made or received by the user from August 1, 2017 to present, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

g. All "check ins" and other location information;

h. All IP logs, including all records of the IP addresses that logged into the account;

i. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

j. All information about the Facebook pages that the account is or was a "fan" of;

k. All past and present lists of friends created by the account;

l. All records of Facebook searches performed by the account from August 1, 2017 to present;

m. All information about the user's access and use of Facebook Marketplace;

n. The types of service utilized by the user;

o. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

p. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

q. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

1. All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of offenses involving providing or attempting to provide material support or resources to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B, occurring from August 1, 2017, to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following:

a. Email, text and other messages, photos, videos, contacts and contact lists, addresses and address books, voicemail messages, location data, calendar, applications and application data, settings;

b. Records and information relating to ISIS, or other foreign terrorist organizations;

c. Records and information relating to the provision, or attempted provision, of material support or resources to ISIS, or other foreign terrorist organizations;

d. Records and information relating to travel, including travel plans, itineraries, reservations, bookings, tickets, and the means and sources of payment for travel;

e. Records and information relating to plans to commit a terrorist attack, or to fight with ISIS, or other foreign terrorist organizations, including, without limitation, funding, materials needed, maps, disguises, aliases, weapons, or the other materials that may assist with such an attack;

f. Records and information relating to communications with others relating to ISIS, or other foreign-terrorist organizations, or potential terrorist attacks on the United States, or in other countries;

g. Records and information relating to the use of YouTube, Facebook, WhatsApp, and other forms of social media, use of the internet, and communication methods, including private messaging;

h. Records and information relating to videos or other content created, publicly posted, or viewed on the internet relating to ISIS, or other foreign-terrorist organizations;

i. Information relating to the communication between account users and other individuals, including potential co-conspirators, accomplices, and associates, relating to ISIS, or other foreign-terrorist organizations, or relating to providing, or attempting to provide, material support or resources for such organizations;

j. Information relating to the identification and contact information of co-conspirators and other individuals engaged or otherwise involved in providing, or

attempting to provide, material support or resources to ISIS, or other foreign-terrorist organizations;

k. Information relating to the timing of communications among coconspirators and other individuals engaged, or otherwise involved, in providing, or attempting to provide, material support or resources to a foreign-terrorist organization;

l. Information relating to the methods and techniques used in providing, or attempting to provide, material support or resources to a foreign-terrorist organization;

m. Information relating to the distribution of videos and photographs evidencing the work, accomplishments, or propaganda of a foreign-terrorist organization;

n. Information relating to the recruitment of additional fighters, supporters, and financial support for a foreign-terrorist organization;

o. Evidence indicating how and when the Facebook account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

p. Records and information indicating the account user's state of mind as it relates to the provision, or attempted provision, of material support or resources to ISIS, or other foreign terrorist organizations;

q. Records of Internet Protocol addresses used;

r. The identity of the person(s) who created, used, or deleted the account, including information that would help reveal the whereabouts of such person;

s. The identity of any person(s) who communicated with the account about matters relating to foreign-terrorist organizations, and any records related to the whereabouts of such persons;

t. Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime; and

u. Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the accounts were activated).

2. Evidence of user attribution showing who used, or owned, the account at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Facebook, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Facebook. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Facebook, and they were made by Facebook as a regular practice; and

b. such records were generated by Facebook's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Facebook in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Facebook, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature